

Oak Ridge National Laboratory

Joint Meeting of
User Facility Administrators
and
User Executive Committee Chairs

Cyber Security Update

*Oak Ridge National Laboratory
March 8, 2005*

OAK RIDGE NATIONAL LABORATORY
U. S. DEPARTMENT OF ENERGY

Cyber Security Update - March 2005

- **Background**
 - DOE National Laboratories and User Facilities
 - Information Technology and Cyber Security
- **Cyber Security Issues 2003 / 2004**
 - Remote Cyber Access
 - Foreign National Access: DOE N 142.3 (draft)
- **Cyber Security Issues 2004 / 2005 +**
 - DOE Office of Science Cyber Security Plan for 2005 (DOE SC slides)
 - Presidents Management Agenda (DOE SC slides)
 - FISMA: Federal Information Security Management Act (DOE SC slides)
 - HSPD-12: PIV – Personal Identity Verification & DOE (DOE SC slides)
 - Foreign National Access: DOE N 142.3 (ORNL)
 - Foreign National Cyber Access directive (draft)

Cyber Security Issues 2004 / 2005 +

DOE Office of Science Cyber Security Plan for 2005 (DOE SC slides)

Cyber Security Issues 2004 / 2005 +

Presidents Management Agenda (DOE SC slides)

Cyber Security Issues 2004 / 2005 +

FISMA: Federal Information Security Management Act (DOE SC slides)

Cyber Security Issues 2004 / 2005 +

HSPD-12: Personal Identity Verification (PIV) (DOE SC slides)

Cyber Security Update - March 2005

(draft ~1/2005) Streamlining Foreign National Access to DOE Unclassified Automated Information Systems (DOE O 205.1-X)

- **Directive development out of the DOE OCIO**
- **Comment coordination between various offices, including NNSA and SC**
 - CI review required
 - Indices checks
 - FACTS will be utilized
 - ID verified
 - Security Plan required
 - Monitoring / Auditing
 - e-signatures and email identifiers
 - No access for sensitive country FN to sensitive systems
 - SME reviews
 - security plans
 - certification and accreditation
 - concurrence by CI and Information Security

ORNL's New Graded Approach for DOE Order 142.3

	Nonsensitive	Sensitive	Terrorist Sensitive
Nonsensitive Information and nonsecure area	<p>~1700 of 2600 (65%)</p> <p>AA, 4 SME & host reviews. No indices req.</p> <p>Entered into FACTS but no AA or SME review No indices req.</p>	<p>~900 of 2600 (34%)</p> <p>AA, 4 SME & host reviews. Completed indices req. for assignees</p> <p>AA, 2 SME, & host review. Completed indices not req.</p>	<p>4 of 2600 (0.1%)</p> <p>Sec. of Energy Approval</p> <p>Sec. of Energy Approval</p>
Sensitive information and secure area	<p>14 of 2600 requests (0.5%)</p> <p>AA, 4 SME & H reviews Completed indices req.</p> <p>AA, 5 SME & H review Completed indices req.</p>	<p>28 of 2600 requests (1%)</p> <p>AA, 4 SME & H reviews Completed indices req.</p> <p>AA, 5 SME & H review Completed indices req.</p>	<p>0 of 2600</p> <p>Sec. of Energy Approval</p> <p>Sec. of Energy Approval</p>

Implementing Graded Approach

		Nonsensitive	Sensitive
GOAL		Entered into FACTS but no AA or SME review. No indices req. ~1700 of 2600 (65%)	AA, 2 SME, & host review. Completed indices not req. ~900 of 2600 (34%)
Nonsensitive Information and nonsecure area		35% of the 1700 eliminated from Export Control by PRA/EXT/Open	42% of 900 eliminated from Export Control
		Export Control will review 65% of the 1700	Export Control will review 58% of the 900
		86% of 1700 Require no Host Agreement	100% of 900 CI needs a Host Agreement (this will be a workflow with about 5 requirements the host will agree to do if the FN accesses the site without completed indices)
		14%*Host Agreement	

* Increased diligence due to CI's counterterrorism requirements for 15 nonsensitive countries

Details of Implementing Graded Approach

		Nonsensitive	Sensitive
GOAL		Entered into FACTS but no AA or SME review. No indices req. ~1700 of 2600 (65%)	AA, 2 SME, & host review. Completed indices not req. ~900 of 2600 (34%)
Nonsensitive Information and nonsecure area		35% of the 1700 eliminated from Export Control by PRA/EXT/Open	42% of 900 eliminated from Export Control
		Export Control will review 65% of the 1700	Export Control will review 58% of the 900
		86% of 1700 Require no Host Agreement	100% of 900 CI needs a Host Agreement (this will be a workflow with about 5 requirements the host will agree to do if the FN accesses the site without completed indices)
		14%*Host Agreement	

* Increased diligence due to CI's counterterrorism requirements for 15 nonsensitive countries